

# Week 8: Simulated Attack & Cloud Incident Response

**Name-** Samruddhi Dattu Nikam

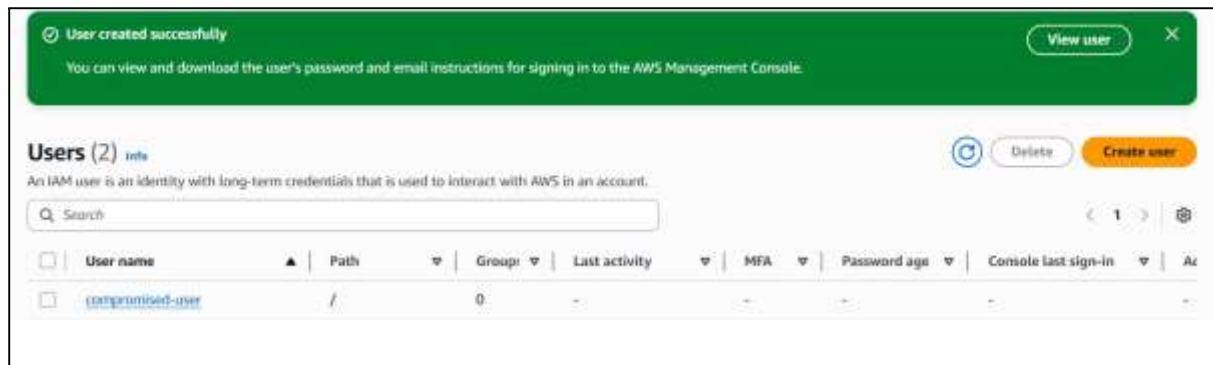
**PRN-** 2124UCSF2019

**Email-** [samruddhi.nikam\\_24ucs@sanjivani.edu.in](mailto:samruddhi.nikam_24ucs@sanjivani.edu.in)

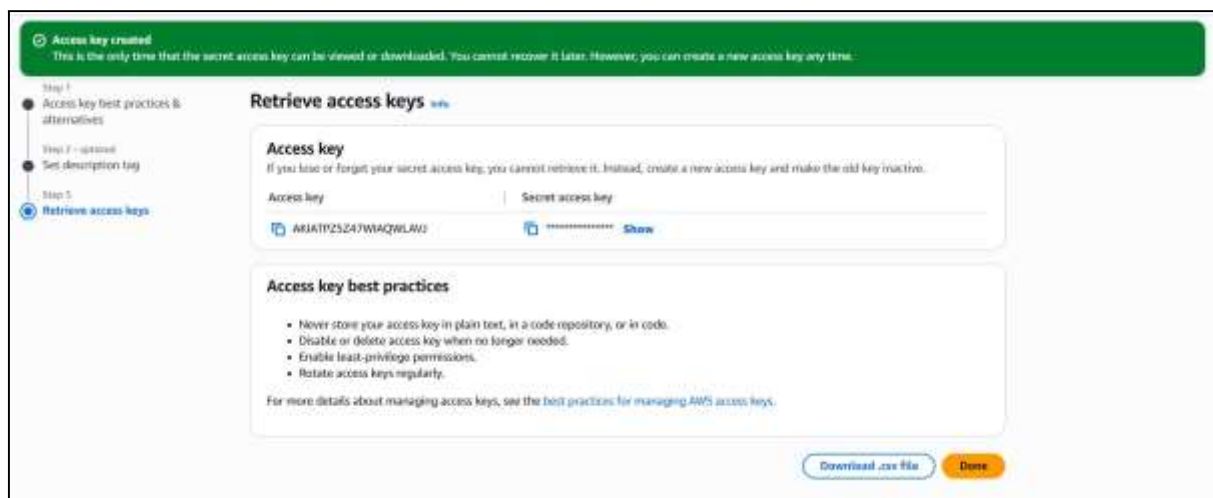
- Task-**
- 1) Simulate a compromised account scenario.
  - 2) Respond & secure the account.
  - 3) Document the incident response steps.

## Task 1- Simulate a Compromised Account.

- 1) Log in to AWS Console. Go to <https://aws.amazon.com>, sign in to the AWS Management Console.
- 2) Create a test IAM user named **compromised-user** with basic permissions (e.g., Amazon S3 read access).



- 3) Generate **Access Keys** for the user.



- 4) Share these keys intentionally with a test machine/script that attempts unauthorized AWS CLI actions (e.g., trying to delete S3 objects without permission).

## Week 8: Simulated Attack & Cloud Incident Response

```
ap-south-1
$ aws s3 ls s3://intern-lab-bucket-11 --profile compromised
ls error occurred (NoSuchBucket) when calling the ListBuckets operation: The specified bucket does not exist
$ aws s3 ls s3://2124mac0811/test.txt --profile compromised
2025-08-18 09:54:41    0 test.txt
$ aws s3 cp s3://intern-lab-bucket-11/test.txt --profile compromised
delete failed: s3://intern-lab-bucket-11/test.txt: An error occurred (NoSuchBucket) when calling the DeleteObject operation: The specified bucket does not exist
$ aws s3 cp s3://2124mac0811/test.txt --profile compromised
delete failed: s3://2124mac0811/test.txt: An error occurred (AccessDenied) when calling the DeleteObject operation: User: arn:aws:iam::240118921788:user/compromised-user is not authorized to perform: s3:DeleteObject on resource: "arn:aws:s3:::2124mac0811/test.txt" because no identity-based policy allows the s3:DeleteObject action
$ clear
$ aws s3 ls s3://2124mac0811 --profile compromised
usage: aws [options] command [subcommand] [subcommand ...] [parameters]
to see help text, you can run:

aws help
aws commands help
aws command [subcommand] help

see: error: argument subcommand: invalid choice, valid choices are:

ls                               | s3help
cp                               | mv
rm                               | sync
mk                               | rb

reassign

$ aws s3 ls s3://2124mac0811 --profile compromised
2025-08-18 09:54:41    0 test.txt
$ aws s3 cp s3://2124mac0811/test.txt --profile compromised
delete failed: s3://2124mac0811/test.txt: An error occurred (AccessDenied) when calling the DeleteObject operation: User: arn:aws:iam::240118921788:user/compromised-user is not authorized to perform: s3:DeleteObject on resource: "arn:aws:s3:::2124mac0811/test.txt" because no identity-based policy allows the s3:DeleteObject action
$ aws s3 cp test.txt s3://2124mac0811 --profile compromised
The user-provided path test.txt does not exist.
$ aws s3 cp test.txt s3://2124mac0811 --profile compromised
The user-provided path test.txt does not exist.
$
```

5) Monitor AWS CloudTrail and CloudWatch to detect unusual activity from the user account.



### Task 2- Respond to the Incident.

1) Identify the Source: Go to CloudTrail → Event History. Filter by compromised-user and check the activity timeline.

```
CloudShell
ap-south-1
$ aws cloudtrail lookup-events \
> --lookup-attributes AttributeKey=Username,AttributeValue=compromised-user \
$ aws cloudtrail lookup-events \
> --lookup-attributes AttributeKey=Username,AttributeValue=compromised-user \
> --max-results 50
{
  "Events": [
    {
      "EventId": "6b3b401f-7f8a-4fc6-9584-890cd06cbf8e",
      "EventName": "ListBuckets",
      "ReadOnly": "true",
      "AccessKeyId": "AKIATP25Z47WIAQMLAVJ",
      "EventTime": "2025-08-18T08:19:54+00:00",
      "EventSource": "s3.amazonaws.com",
      "Username": "compromised-user",
      "Resources": [],
      "CloudTrailEvent": "{\"eventVersion\":\"1.11\",\"userIdentity\":{\"type\":\"IAMUser\",\"principalId\":\"AIDATP25Z47WIAQMLAVJ\",\"arn\":\"arn:aws:iam::240118921788:user/compromised-user\",\"accountId\":\"24:...skipping...\"}"
    }
  ]
}
```

2) Secure the Account: Deactivate the compromised Access Keys: `aws iam update-access-key --access-key-id <ACCESS_KEY> --status Inactive --user-name compromised-user`

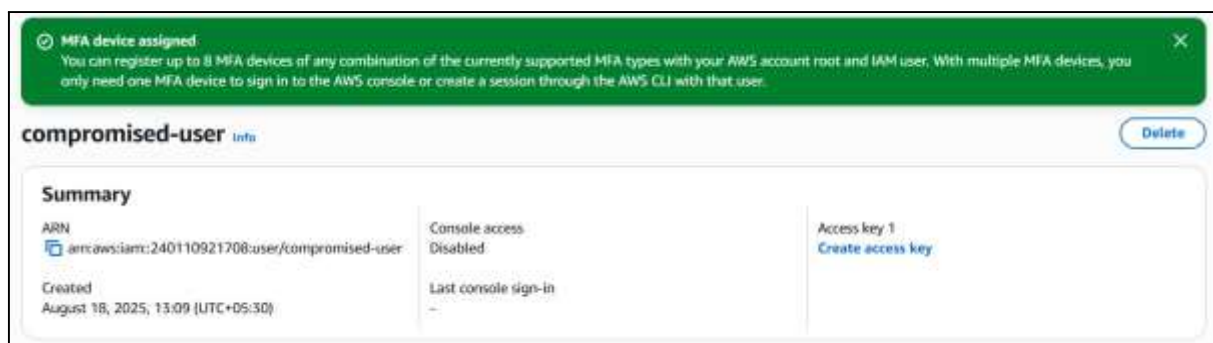
## Week 8: Simulated Attack & Cloud Incident Response

```
~ $
~ $ aws iam list-access-keys --user-name compromised-user
{
  "AccessKeyMetadata": [
    {
      "UserName": "compromised-user",
      "AccessKeyId": "AKIATPZ5Z47WIAQWLAVJ",
      "Status": "Active",
      "CreateDate": "2025-08-18T07:40:51+00:00"
    }
  ]
}
~ $ for AKI in $(aws iam list-access-keys --user-name compromised-user \
> --query 'AccessKeyMetadata[].AccessKeyId' --output text); do
> aws iam update-access-key --user-name compromised-user \
> --access-key-id $AKI --status Inactive
> done
~ $ for AKI in $(aws iam list-access-keys --user-name compromised-user \
> --query 'AccessKeyMetadata[].AccessKeyId' --output text); do
> aws iam delete-access-key --user-name compromised-user --access-key-id $AKI
> done
~ $ aws iam delete-login-profile --user-name compromised-user
```

3) Restrict Permissions: Detach all policies from the user. Remove from any IAM group.

```
~ $
~ $ for ARN in $(aws iam list-attached-user-policies --user-name compromised-user \
> --query 'AttachedPolicies[].PolicyArn' --output text); do
> aws iam detach-user-policy --user-name compromised-user --policy-arn $ARN
> done
~ $ for NAME in $(aws iam list-user-policies --user-name compromised-user \
> --query 'PolicyNames[]' --output text); do
> aws iam delete-user-policy --user-name compromised-user --policy-name $NAME
> done
~ $ for G in $(aws iam list-groups-for-user --user-name compromised-user \
> --query 'Groups[].GroupName' --output text); do
> aws iam remove-user-from-group --group-name $G --user-name compromised-user
> done
~ $
```

4) Enable MFA (Multi-Factor Authentication) on the account.



### Task 3- Document the Incident Response Steps.

#### Incident Summary:

- **Incident Type:** Simulated account compromise.
- **Impact:** Unauthorized S3 deletion attempt blocked.
- **Detection Method:** AWS CloudTrail & CloudWatch alerts.
- **Response Actions:** Access keys deactivated, permissions removed, MFA enabled.